December 2019

ANALYZING AND ARTICULATE RULE PERFORMANCE TO INCREASE EFFICIENCY

Pradipta Das Sarkar

ANALYZING AND ARTICULATE RULE PERFORMANCE TO INCREASE EFFICIENCY

AUTHOR:

Pradipta Das Sarkar

ABSTRACT

Presented herein are techniques for overlaying policy modification into historical rule hits and events to enable an administrator to visualize changes that have caused traffic matches to go up and/or down. This visualization, sometimes referred to herein as the visualization of a "Rule Heartbeat," provides a new dimension in network security that facilitates optimization of network polices, but also elevates the experience in the network security ecosystem.

DETAILED DESCRIPTION

In the network security eco-system, monitoring and managing of rule usage in devices is very critical. For example, over a period of time, firewall rule bases can become inefficient as rules become disorganized, causing some rules to become ineffective. This primarily occurs because of a lack of timely notification to end users when new rules, or changed rules, are added, which can adversely affect other rules in the rule base. This, in turn, leads to device performance issues and can be a problem for end users. Conventional approaches to monitoring and managing of rule usage lack any type of mechanism that can be used to analyze policies and explore the redundant anomalies in a rule.

As such, presented herein are techniques that empower an administrator to visualize the anomalies in a rule from the policy table itself and enable the administrator to optimize the rule base (e.g., firewall rule base). In particular, this new visualization mechanism, sometimes referred to herein as the visualization of a “Rule Heartbeat,” includes the rule history, hit counts and events in one plane for better articulation. The visualization provides an overview of all the rule activities which is pinned with the rule timeline. The timeline also projects the historical hit counts of all the shared devices, as well as the events, occurred due to this rule. These capabilities enable an administrator to visualize the

changes that, for example, have caused traffic matches to go up and/or down and, accordingly, enable the administrator to optimize the associated policy/policies.

The visualization techniques presented herein provide the ability to quickly obtain a snapshot of the critical events being in the context. The visualization techniques also provide a list of individual devices, as well as the rule(s) shared with and their respective rule hit counts. The visualization techniques further provide a snapshot of the objects, the rule(s) that the objects are using, and their individual participation to this rule by providing a hit counts. The visualization techniques also provide a quick analysis of hits and events, and the snapshot concludes with a rule usage percentage and identification of devices that are assigned with a rule, but not in use.

FIGs. 1-5, below, provide a product design specification for the visualization techniques presented herein.

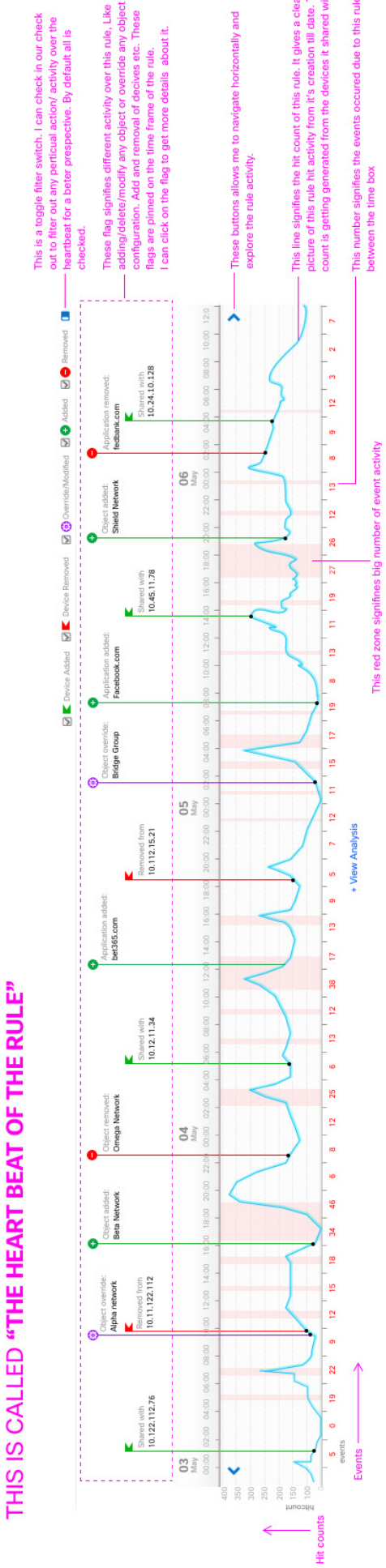
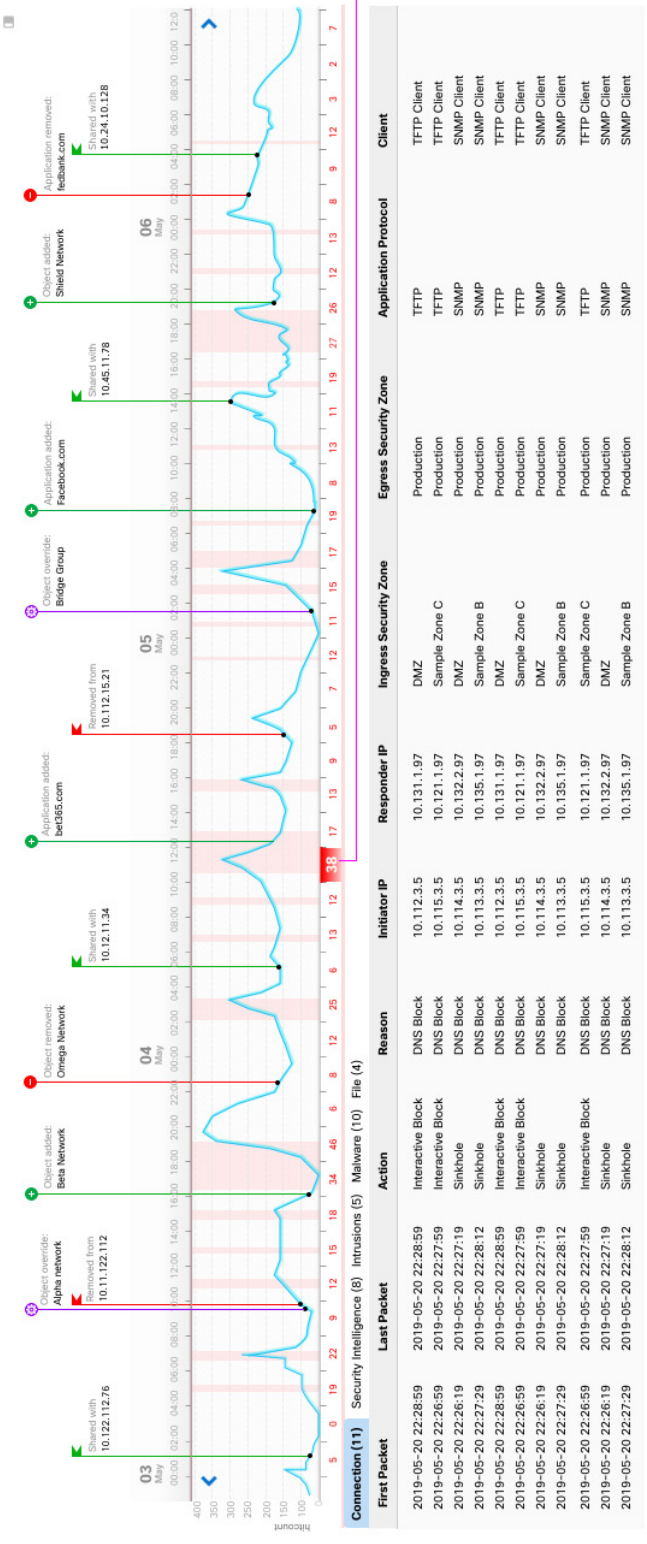

THIS IS CALLED "THE HEART BEAT OF THE RULE"
This is a toggle filter switch. I can check in our check out to filter out any perticual action/ activity over the heartbeat for a beter prespective. By default all is checked.
These flag signifies different activity over this rule. Like adding/delete/modify any object or override any object configuration. Add and removal of decives etc. These flags are pinned on the time frame of the rule. I can click on the flag to get more details about it.
These buttons allows me to navigate horizontally and explore the rule activity.
This line signifies the hit count of this rule. It gives a clear picture of this rule hit activity from it's creation till date. This count is getting generated from the devices it shared with.
This number signifies the events occured due to this rule between the time box
This red zone signifines big number of event activity
Device Added
Device Removed
Override/Modified
Added
Removed
Object override: Alpha network
Removed from 10.11.122.112
Shared with 10.122.112.76
Object added: Beta Network
Object removed: Omega Network
Shared with 10.12.11.34
Application added: bet365.com
Removed from 10.112.15.21
Object override: Bridge Group
Application added: Facebook.com
Shared with 10.45.11.78
Object added: Shield Network
Application removed: fedbank.com
Shared with 10.24.10.128
03 May
04 May
05 May
06 May
+ View Analysis
Events
Hit counts

FIG. 1

FIG. 2



Connection (11) | Security Intelligence (8) | Intrusions (5) | Malware (10) | File (4)

First Packet	Last Packet	Action	Reason	Initiator IP	Responder IP	Ingress Security Zone	Egress Security Zone	Application Protocol	Client
2019-05-20 22:28:59	2019-05-20 22:28:59	Interactive Block	DNS Block	10.112.3.5	10.131.1.97	DMZ	Production	TFTP	TFTP Client
2019-05-20 22:26:59	2019-05-20 22:27:59	Interactive Block	DNS Block	10.115.3.5	10.121.1.97	Sample Zone C	Production	TFTP	TFTP Client
2019-05-20 22:26:19	2019-05-20 22:27:19	Sinkhole	DNS Block	10.114.3.5	10.132.2.97	DMZ	Production	SNMP	SNMP Client
2019-05-20 22:27:29	2019-05-20 22:28:12	Sinkhole	DNS Block	10.113.3.5	10.135.1.97	Sample Zone B	Production	SNMP	SNMP Client
2019-05-20 22:28:59	2019-05-20 22:28:59	Interactive Block	DNS Block	10.112.3.5	10.131.1.97	DMZ	Production	TFTP	TFTP Client
2019-05-20 22:26:59	2019-05-20 22:27:59	Interactive Block	DNS Block	10.115.3.5	10.121.1.97	Sample Zone C	Production	TFTP	TFTP Client
2019-05-20 22:26:19	2019-05-20 22:27:19	Sinkhole	DNS Block	10.114.3.5	10.132.2.97	DMZ	Production	SNMP	SNMP Client
2019-05-20 22:27:29	2019-05-20 22:28:12	Sinkhole	DNS Block	10.113.3.5	10.135.1.97	Sample Zone B	Production	SNMP	SNMP Client
2019-05-20 22:26:59	2019-05-20 22:27:59	Interactive Block	DNS Block	10.115.3.5	10.121.1.97	Sample Zone C	Production	TFTP	TFTP Client
2019-05-20 22:26:19	2019-05-20 22:27:19	Sinkhole	DNS Block	10.114.3.5	10.132.2.97	DMZ	Production	SNMP	SNMP Client
2019-05-20 22:27:29	2019-05-20 22:28:12	Sinkhole	DNS Block	10.113.3.5	10.135.1.97	Sample Zone B	Production	SNMP	SNMP Client

FIG. 3

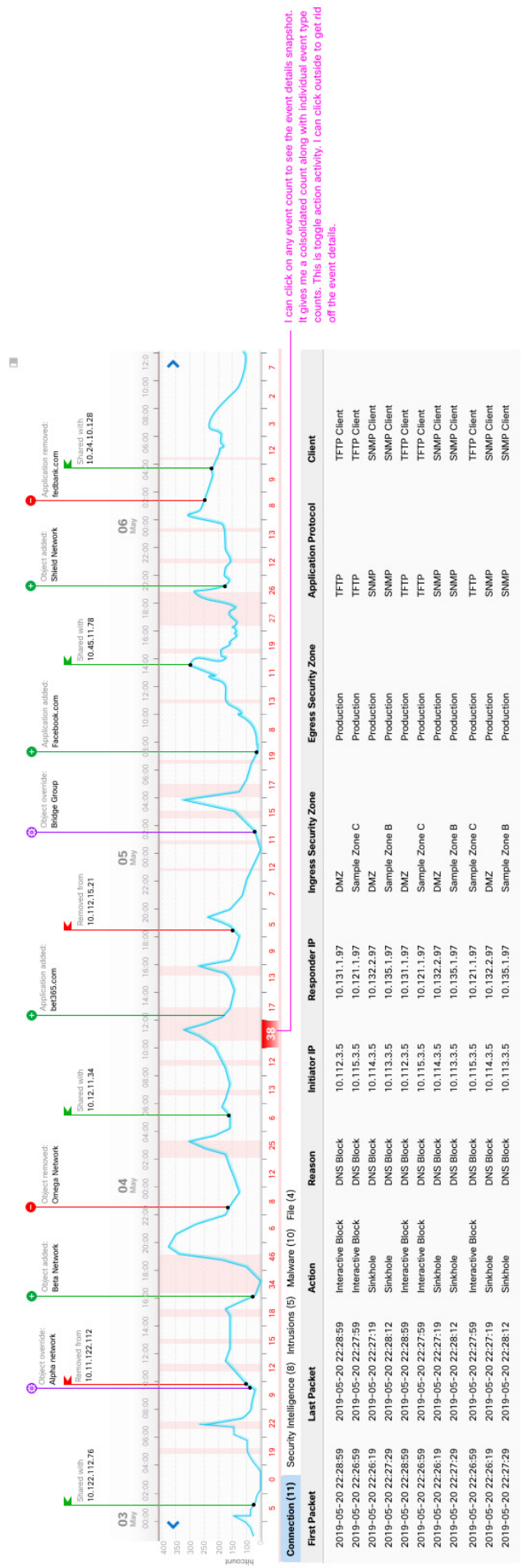

I can click on any event count to see the event details snapshot. It gives me a colsolidated count along with individual event type counts. This is toggle action activity. I can click outside to get rid off the event details.
Connection (11) Security Intelligence (8) Intrusions (5) Malware (10) File (4)
First Packet | Last Packet | Action | Reason | Initiator IP | Responder IP | Ingress Security Zone | Egress Security Zone | Application Protocol | Client
2019-05-20 22:28:59 | 2019-05-20 22:28:59 | Interactive Block | DNS Block | 10.112.3.5 | 10.131.1.97 | DMZ | Production | TFTP | TFTP Client
2019-05-20 22:26:59 | 2019-05-20 22:27:59 | Interactive Block | DNS Block | 10.115.3.5 | 10.121.1.97 | Sample Zone C | Production | TFTP | TFTP Client
2019-05-20 22:26:19 | 2019-05-20 22:27:19 | Sinkhole | DNS Block | 10.114.3.5 | 10.132.2.97 | DMZ | Production | SNMP | SNMP Client
2019-05-20 22:27:29 | 2019-05-20 22:28:12 | Sinkhole | DNS Block | 10.113.3.5 | 10.135.1.97 | Sample Zone B | Production | SNMP | SNMP Client
2019-05-20 22:28:59 | 2019-05-20 22:28:59 | Interactive Block | DNS Block | 10.112.3.5 | 10.131.1.97 | DMZ | Production | TFTP | TFTP Client
2019-05-20 22:26:59 | 2019-05-20 22:27:59 | Interactive Block | DNS Block | 10.115.3.5 | 10.121.1.97 | Sample Zone C | Production | TFTP | TFTP Client
2019-05-20 22:26:19 | 2019-05-20 22:27:19 | Sinkhole | DNS Block | 10.114.3.5 | 10.132.2.97 | DMZ | Production | SNMP | SNMP Client
2019-05-20 22:27:29 | 2019-05-20 22:28:12 | Sinkhole | DNS Block | 10.113.3.5 | 10.135.1.97 | Sample Zone B | Production | SNMP | SNMP Client
2019-05-20 22:26:59 | 2019-05-20 22:27:59 | Interactive Block | DNS Block | 10.115.3.5 | 10.121.1.97 | Sample Zone C | Production | TFTP | TFTP Client
2019-05-20 22:26:19 | 2019-05-20 22:27:19 | Sinkhole | DNS Block | 10.114.3.5 | 10.132.2.97 | DMZ | Production | SNMP | SNMP Client
2019-05-20 22:27:29 | 2019-05-20 22:28:12 | Sinkhole | DNS Block | 10.113.3.5 | 10.135.1.97 | Sample Zone B | Production | SNMP | SNMP Client

FIG. 4

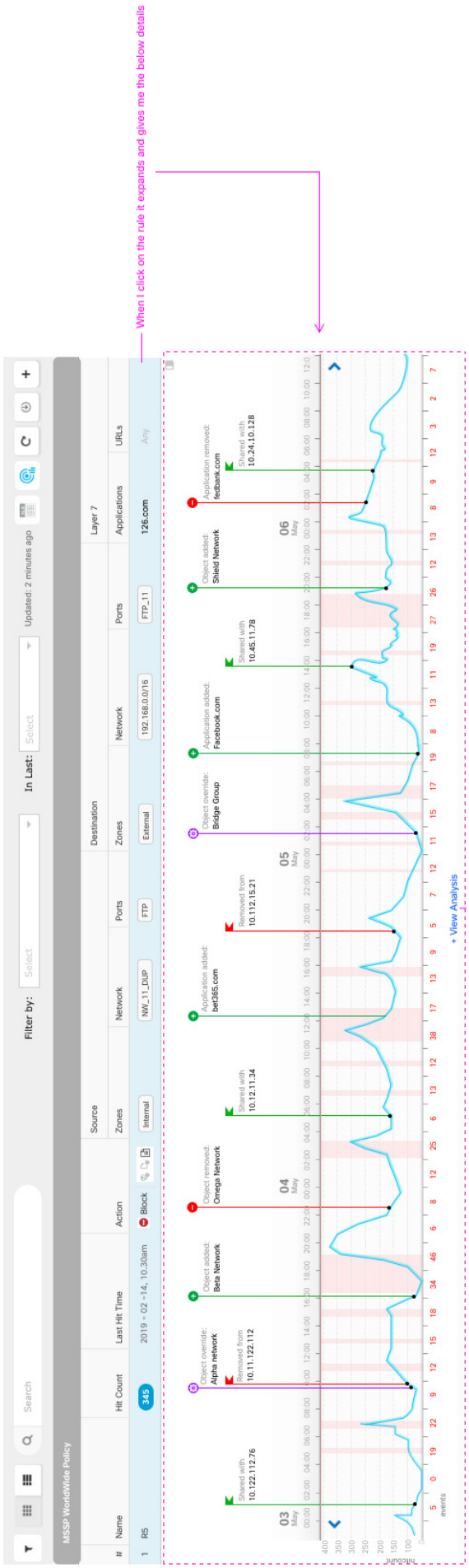
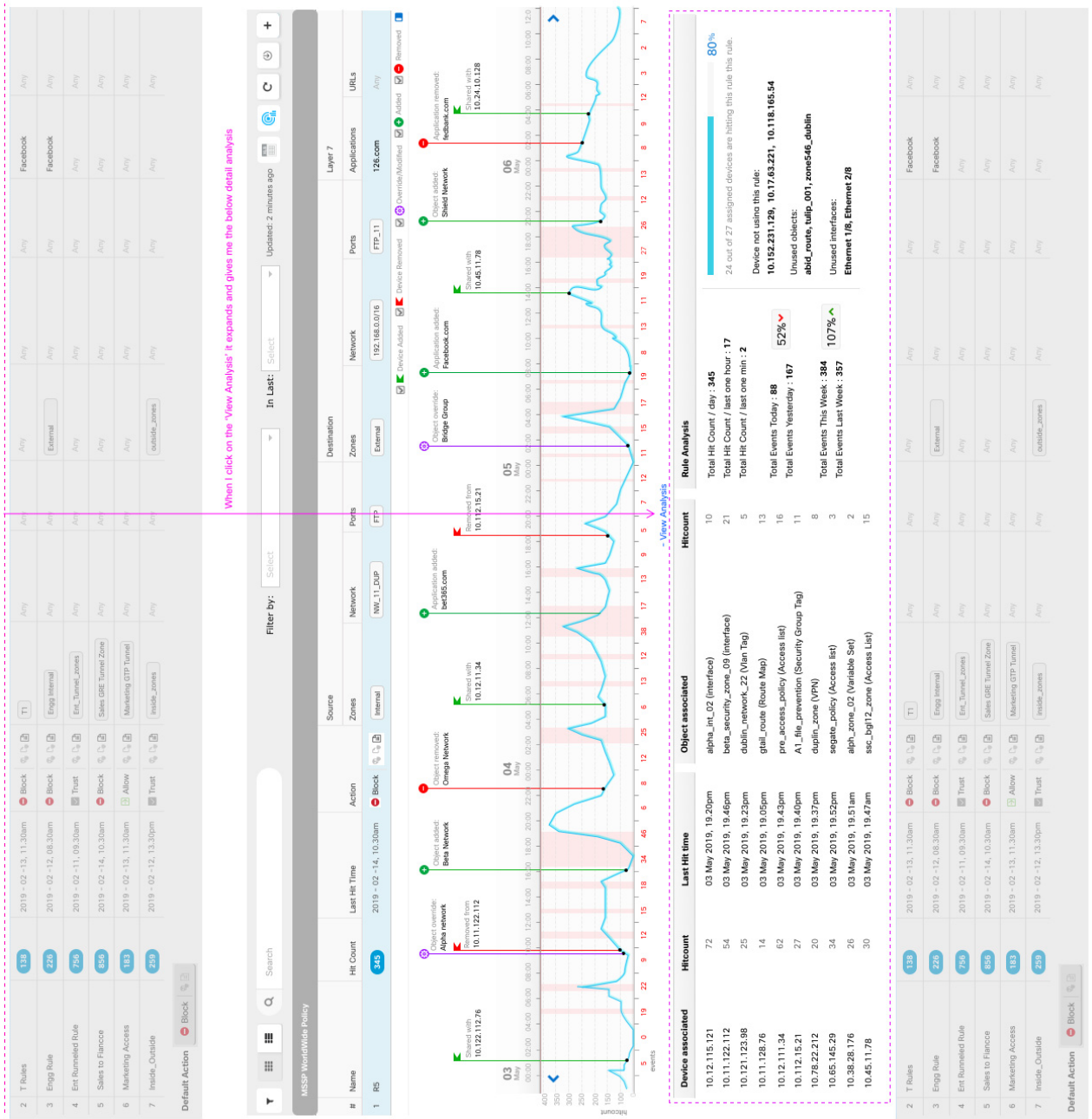

When I click on the rule it expands and gives me the below details
MSSP WorldWide Policy
Search
Filter by:
Select
In Last:
Select
Updated: 2 minutes ago
Name
Hit Count
Last Hit Time
Action
Source
Destination
Layer 7
Zones
Network
Ports
Zones
Network
Ports
Applications
URLs
R5
345
2019 - 02 - 14, 10.30am
Block
Internal
NW_11_DUP
FTP
External
192.168.0.0/16
FTP_11
126.com
Any
Object override: Alpha network
Removed from 10.11.122.112
Shared with 10.122.112.76
Object added: Beta Network
Object removed: Omega Network
Shared with 10.12.11.34
Application added: bet365.com
Removed from 10.112.15.21
Object override: Bridge Group
Application added: Facebook.com
Shared with 10.45.11.78
Object added: Shield Network
Application removed: fedbank.com
Shared with 10.24.10.128
03 May
04 May
05 May
06 May
+ View Analysis
Hitcount
events

FIG. 5


When I click on the 'View Analysis' it expands and gives me the below detail analysis
MSSP WorldWide Policy
Filter by:
In Last:
Updated: 2 minutes ago
View Analysis
Rule Analysis
Total Hit Count / day : 345
Total Hit Count / last one hour : 17
Total Hit Count / last one min : 2
Total Events Today : 88
Total Events Yesterday : 167
52%
Total Events This Week : 384
Total Events Last Week : 357
107%
24 out of 27 assigned devices are hitting this rule this rule.
Device not using this rule:
10.152.231.129, 10.17.63.221, 10.118.165.54
Unused objects:
abid_route, tulip_001, zone546_dublin
Unused interfaces:
Ethernet 1/8, Ethernet 2/8